

山东威高集团医用高分子制品股份有限公司
Shandong Weigao Group Medical Polymer Company Limited

信息安全政策
Information Security Policy

1. 目的和原则 | Purpose and Principles

适用实体承诺保护信息和系统的机密性、完整性、可用性和隐私，持续改进信息安全管理，监测并响应威胁，并明确全体员工及第三方的责任。

The Reporting Entities are committed to protecting the confidentiality, integrity, availability and privacy of information and systems; continually improving information-security management; monitoring and responding to threats; and defining responsibilities for the entire workforce and third parties.

2. 适用范围 | Scope

除非相关政策另有说明，本政策适用于山东威高集团医用高分子制品有限公司、其于中国成立的附属公司以及在报告边界内的美国介入医疗产品制造业务（统称“适用实体”）。

Unless otherwise stated, this Policy applies to Shandong Weigao Group Medical Polymer Company Limited, its PRC subsidiaries Argon Medical's US interventional medical products manufacturing business within the reporting boundary (collectively, the "Reporting Entities").

本政策覆盖所有信息、纸质和电子记录、企业系统、云服务、网络、终端、生产控制系统、实验室系统、客户服务工具、网站以及联网医疗器械或相关软件（如适用）。

This Policy covers all information, paper and electronic records, enterprise systems, cloud services, networks, endpoints, manufacturing-control systems, laboratory systems, customer-service tools, websites and connected medical devices or related software, where applicable.

3. 治理与风险管理 | Governance and Risk Management

- 执行管理层或其指定的管理委员会负责监督信息安全治理，定期审阅重大信息安全风险、事件、整改措施及资源需求，并视需要向董事会或其授权委员会报告。执行管理层应指定一名对信息安全负有明确责任的高级负责人。IT 部门负责信息安全控制措施的日常实施与维护；法务及隐私、质量、监管事务和各业务负责人共同管理相关合规、患者安全、产品质量及业务风险。
Executive management, or a management committee designated by it, shall oversee information security governance, periodically review material information security risks, incidents, remediation actions and resource requirements, and report to the Board or an authorised Board committee where appropriate. Executive management shall designate a senior leader with clear accountability for information security. The IT function shall be responsible for the day-to-day implementation and maintenance of information security controls, while Legal and Privacy, Quality, Regulatory Affairs and relevant business owners shall jointly manage associated compliance, patient safety, product quality and business risks.
- 至少每年以及在重大系统、收购、供应商、产品或威胁变化时开展信息安全风险评估，并将高风险纳入整改计划和管理层报告。
Information-security risk assessments shall be conducted at least annually and following material changes in systems, acquisitions, suppliers, products or threats, with high risks included in remediation plans and management reporting.
- 建立信息资产清单、数据分类、系统负责人和风险接受程序。
Maintain information-asset inventories, data classification, system ownership and formal risk-acceptance procedures.

4. 访问、系统和数据保护 | Access, Systems and Data Protection

- 按照最小权限、知情需要和职责分离原则管理账户；对高风险和远程访问采用多因素认证；及时审查和撤销离职、转岗或不再需要的访问。
Manage accounts according to least privilege, need to know and segregation of duties; apply multi-factor authentication to high-risk and remote access; and promptly review and revoke access following departure, role change or loss of need.

- 根据风险采用加密、备份、日志、恶意软件防护、网络分段、安全配置、补丁、漏洞扫描和渗透测试。
Use encryption, backup, logging, malware protection, network segmentation, secure configuration, patching, vulnerability scanning and penetration testing according to risk.
- 软件开发、系统变更和联网医疗器械（如适用）应实施安全设计、代码和架构审查、测试、漏洞处理、发布控制及上市后监测。
Software development, system change and connected medical devices, where applicable, shall apply security by design, code and architecture review, testing, vulnerability handling, release control and post-market monitoring.

5. 第三方和云服务 | Third Parties and Cloud Services

在供应商接入系统或处理敏感信息前，应开展风险分级和安全尽职调查，在合同中规定保密、访问、事件通知、审计、分包、数据位置、删除及业务连续性要求，并定期复审高风险供应商。

Before a supplier accesses systems or processes sensitive information, risk-tiering and security due diligence are required. Contracts must address confidentiality, access, incident notification, audit, subcontracting, data location, deletion and business continuity, with periodic review of high-risk suppliers.

6. 事件响应和业务连续性 | Incident Response and Business Continuity

- 建立 24 小时或适当时效的信息安全事件报告、分级、遏制、调查、恢复、证据保全、根本原因分析和纠正措施流程，并依法通知客户、个人、监管机关或其他相关方。
Maintain timely, including 24-hour where appropriate, processes for reporting, classifying, containing, investigating and recovering from information-security incidents, preserving evidence, analysing root cause and implementing corrective action, with lawful notification to customers, individuals, regulators or others.
- 建立业务影响分析、业务连续性计划和灾难恢复计划，明确关键流程、恢复时间和恢复点目标、替代安排、备份测试及定期演练。
Maintain business-impact analyses, business-continuity plans and disaster-recovery plans defining critical processes, recovery-time and recovery-point objectives, alternatives, backup testing and periodic exercises.
- 可能影响医疗器械安全、性能、监管义务或患者安全的网络安全事件须同步升级至质量和监管事务职能。
Cybersecurity incidents that may affect medical-device safety, performance, regulatory duties or patient safety must also be escalated to Quality and Regulatory Affairs.

7. 人员、监测和审计 | People, Monitoring and Audit

- 所有员工应接受入职及年度信息安全培训；高权限、研发、IT、客户服务和处理敏感数据的人员应接受岗位专项培训和模拟测试。违规可导致访问撤销、纪律处分或第三方终止。
All employees shall receive induction and annual information-security training. Privileged users and personnel in R&D, IT, customer service or sensitive-data processing shall receive role-specific training and simulations. Breaches may result in access revocation, disciplinary action or third-party termination.
- 适用实体应进行日志和威胁监测、漏洞管理、内部审计及风险导向的独立评估，并披露适用的 ISO/IEC 27001 或其他认证状态，不得暗示未取得认证。
The Reporting Entities shall conduct logging and threat monitoring, vulnerability management, internal audit and risk-based independent assessment, and disclose applicable ISO/IEC 27001 or other certification status without implying certification that has not been obtained.